Summary of Harris Corporation Comments on Cybersecurity Issues
Before the Federal Communications Commission
Ex Parte Presentation

October 20, 2010

I. Effects of Broadband Communications Networks of Damage to or Failure of Network Equipment or Severe Overload (PS Docket 10-92)

Harris Reply Comment Submitted September 3, 2010

<u>Single Points of Failure</u>

- Many physical communications paths (fiber and copper) and physical buildings along major lines of communications are vulnerable to network failure and a potential source of single points of failure, especially at a network's edge.
  - Sabotage
  - Severed Lines of Connectivity
  - Co-location Issues
  - Electrical Grid Failures
- Best assurance of survivability in these scenarios is the use of two or more dissimilar paths to route the same information.

<u>Ensuring Redundancy</u>

- The Commission must cultivate its working relationships with private industry, standard setting organizations, and other government agencies.
  - Participation in interagency organizations and working groups.
  - Adoption of a set of <u>voluntary</u> guidelines or Industry Best Practices that would be used to help broadband network operators oversee and achieve appropriate levels of redundancy in broadband communications networks.

<u>Network Design to Prevent Overloads and Points of Failure</u>

- Communications infrastructure is economically sized to carry a fraction of the total potential traffic. It is essential that strategically important broadband networks are designed for as much as one hundred and twenty-five percent of maximum peak traffic.
  - While this concept may not be economically efficient and practical in a straight commercial environment, such a design is critical to many strategically important government, critical infrastructure, and first responder broadband networks.
- Precautions can be taken to maintain a broadband network's functionality and prevent overloading in the event of a disaster including:
  (1) Updating critical router software;
  (2) Employing network monitoring;
  (3) Inclusion of an edge gateway device for automatic detection of anomalous network/packet activity;
  (4) Incorporating trusted priority over-ride codes; and
  (5) For networks carrying mission critical communications, maintaining a backup operations center(s) at dissimilar locations, along with dual routing of network management information from critical network nodes to the network control centers.

II. Cyber Security Certification Program (PS Docket No. 10-93)

Harris Reply Comment Submitted September 8, 2010

A Voluntary Certification Program Will Be Resource Intensive and Difficult to Maintain

- The overhead necessary for the Commission to track potentially thousands of certifications would likely demand an extremely large amount of human and financial capital, including training, database creation and maintenance, data storage and archiving, project planning, certification application tracking, and program compliance.
- Keeping up with changes in security procedures and threats to keep a certification program relevant will require a significant commitment of resources.
    - Efforts may be more appropriately undertaken by industry or independent third party vendors, as opposed to the government.

Commission Action May Mitigate Efforts Already Being Undertaken

- Existing industry efforts, both independent and public-private partnerships, provide diverse solution sets to addressing current and emerging cyber security challenges.
- A process driven by specific industries will provide the flexibility needed to take into account the diverse nature of addressing modern cyber security issues and help promote innovative solutions to addressing new cyber security threats.
    - From a practical level it would be difficult for a government run certification scheme to provide the flexibility necessary to address current and emerging threats
    - There is no "one size fits all" approach to cyber security.
- The Commission may be better served at this time by continuing to emphasize compliance with standard setting bodies, conducting periodic reviews of the state of the cyber security industry, interfacing with other government agencies to create uniform standards, and taking steps to promote a culture of diligent and informed cyber security practices amongst consumers. Actions that can be taken include:
    1. Leveraging its purchasing power to create incentives for companies that do business with the government to adopt high level cyber security practices;
    2. Extending grants to companies developing and implementing cyber security technologies and practices; and
    3. Harmonizing cyber security policy and efforts to eliminate inefficiencies or redundancies.

III. National Broadband Plan Recommendation to Create a Cybersecurity Roadmap (PS Docket No. 10-146)

Harris Comment Submitted September 23, 2010

Key Cybersecurity Vulnerabilities that Should be Addressed

- End users are unfamiliar with security policies, do not understand why practices must be followed, and are generally uneducated about basic cybersecurity best practices.
    - Lack of user education consists both of a lack of knowledge of security protocols and a lack of understanding as to why on-line security protocols are necessary.
- The nation's IT and IA workforce must develop critical cybersecurity skill sets and maintain those skill sets to address key network vulnerabilities
    - The Commission should encourage industry, government, and academia to establish incentives for those employees to be trained, and promote economic and honorary incentives.
- Within many enterprises' IT infrastructure there is insufficient supply chain integrity, both on the software and hardware level, and a lack of continuous network oversight.
    - The Commission should encourage additional network monitoring and oversight on a continuous basis through enhanced software and hardware monitoring that can be used to identify changes in configuration and data integrity.

The Commission Should Coordinate Its Cybersecurity Efforts

- In order to ensure Commission initiatives do not contradict or mitigate other ongoing cybersecurity efforts, the Commission must take into consideration the efforts of other government entities as well as private industry, before taking action, such as:.
    - Working with its federal partners to encourage mid level and senior government IT security subject matter experts to engage with subject matter experts across industry;
    - Coordinating with other government partners on what role the Commission is best suited to perform within existing efforts;
    - Facilitating an understanding among stakeholders of existing domestic and international laws, agency and executive directives, and other notable government and industry policies.
- The Commission in its Cybersecurity Roadmap should increase mitigation efforts and help ensure the confidentiality, integrity, authentication, and availability of communications networks and user data through:
    - Widespread adoption of trusted computing technologies;
    - Engagement with industry, academia, and government bodies in crafting policies:
    - Ongoing development of cybersecurity "communities of interest;"
    - Implementing rapid non-attributable reporting methods by stakeholders of new and existing vulnerabilities.
    - Promoting continuous monitoring in real time, as opposed to periodic reporting.
    - Encouraging internal auditing and reporting of information technology environment scans, breaches, and actions; and
    - Use of existing information assurance programs and new third party vendor offerings to oversee, monitor, and confirm the use of appropriate cybersecurity protocols, both preventative and reactive.